RE: *Indicator Suspcious* URL/Domain/IP Assessment Report - 193960

Yogesh Gholap <yogesh.gholap@tcs.com>

Tue 01/03/2022 11:44 AM

To: InternalIS SecOpsL2Support <InternalIS.SecOpsL2Support@tcs.com>

Cc: InternalIS CyberSecurityops <internalis.cybersecurityops@tcs.com>

Approved to unblock as it has low risk score and domain is not malicious as such.

Best Regards
Yogesh Shantaram Gholap
CSOC Manager, CyberSecurity
Internal IT Infrastructure Services
Tata Consultancy Services
Olympus, Rodas Enclave,
Hiranandani Estate.
Thane West - 400607
Maharashtra, India.
Extn:- 14238
Ph:- 912263714238
Buzz:- 4274238
Cell:- 9930791585
InternalIS CyberSecurity Team 24*7 number - Pstn - +912263718870, Voip 4278870, Extn 18870(Extn is for Mumbai Offices Only)
Mailto: yogesh.gholap@tcs.com
Website: http://www.tcs.com

From: Suhas Wadia <wadia.suhas@tcs.com> **On Behalf Of** InternalIS CyberSecurityops
Sent: Thursday, February 24, 2022 10:55 PM
To: Yogesh Gholap <yogesh.gholap@tcs.com>
Cc: InternalIS CyberSecurityops <internalis.cybersecurityops@tcs.com>
Subject: Re: *Indicator Suspcious* URL/Domain/IP Assessment Report - 193960

Dear Yogesh sir,

PFB analysis for domain - api.ipify.org

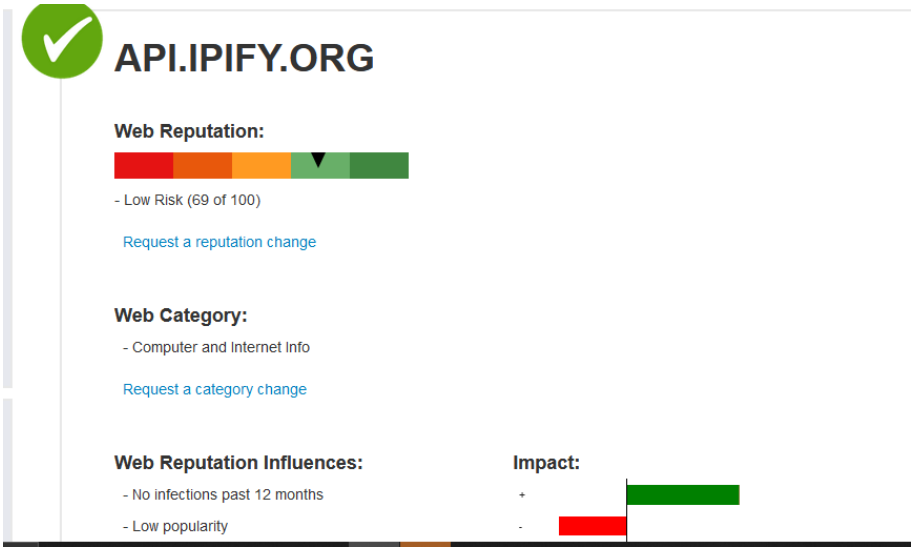
Domain - api.ipify.org
Creation date - 2014-01-05
Reputation - Suspicious

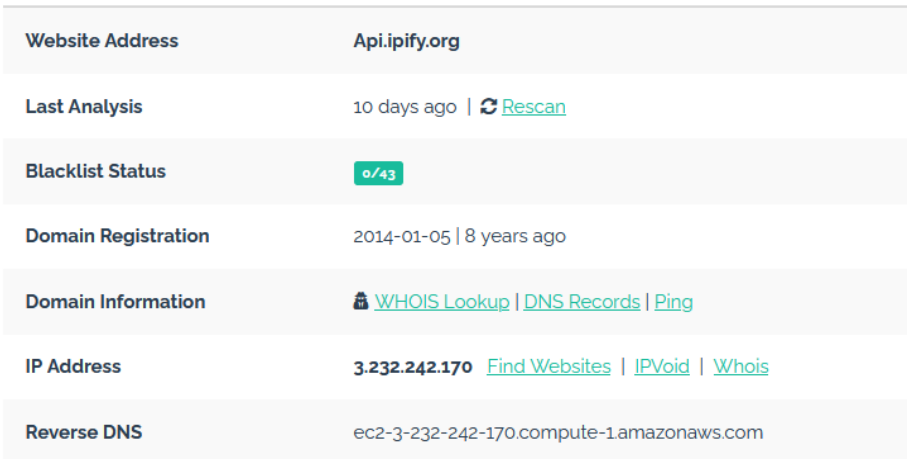
Rf score - 24
Virustotal - 1/90
Urlvoid - clean
Bright cloud - clean

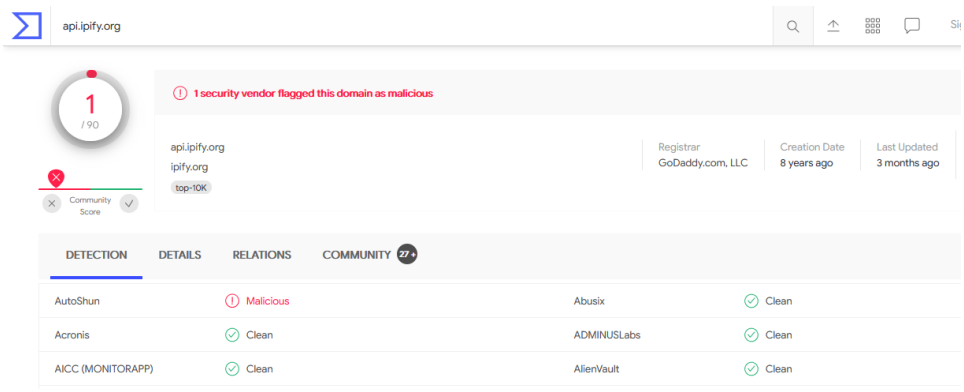
About domain - The domain (api.ipify.org) often appears in IOC lists or is associated with Malware. The site itself is safe to use and has no issues. The site appears in IOC list because it is often abused by malicious sites

or code. The site has an API that is free to use, it will return your IP address, that is why it is used by malicious code.

Kindly suggest, can we unblock this domain ?







TCS Confidential

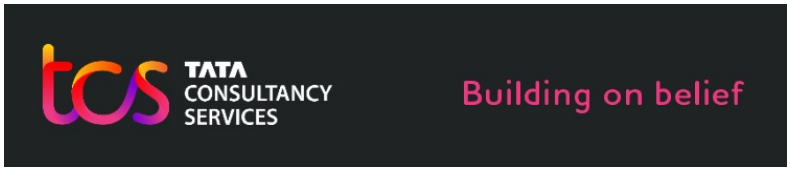
Thanks & Regards
InternalIT Cyber Security Operations
Infrastructure Services, Internal IT
Mumbai,Maharashtra
India
*InternalIS CyberSecurity Team 24*7 number - Pstn - +912263718870, Voip 4278870, Extn 18870(Extn is for Mumbai Offices Only)*
Mailto: internalis.cybersecurity@tcs.com , internalis.cybersecurityops@tcs.com

Escalation Level1: Mr.Yogesh Gholap +91 22 677 99200 yogesh.gholap@tcs.com

---

Experience certainty. IT Services
Business Solutions
Consulting

From: InternalIS CyberAutoBot <InternalIS.CyberAutoBot@tcs.com>
Sent: Thursday, February 24, 2022 9:50 PM
To: Vishwajit Patil <patil.vishwajit@tcs.com>
Cc: InternalIS CyberSecurityops <internalis.cybersecurityops@tcs.com>; Yogesh Gholap <yogesh.gholap@tcs.com>; KUNAL KRUSHEV <kunal.krushev@tcs.com>
Subject: *Indicator Suspcious* URL/Domain/IP Assessment Report - 193960



Hello Human,

My assessment concluded the indicator(s) as **SUSPCIOUS** and needs further investigation.

CSOC Team, please review my report and investigate if the indicators(s) can be allowed on the proxy. Please share results with the CSOC manager.

Investigation Id: 193960

Recorded Future - Domain

Address	Verdict
api.ipify.org	24

Indicators Investigated

Domain	URL
ipify.org, api.ipify.org	https://api.ipify.org/?format=json

Regards,
Cyber AutoBot
Internal IT IS - Cyber Security

Hi,

Kindly validate attached URL

Purpose of url - Simple Public IP Address API
Project Name - Bancolombia ADM - WON 20213368
Location- Medellín - Colombia

Thanks & Regards,

IT Security | Security Operations Support,

Infrastructure Services, Internal IT,

Tata Consultancy Services Limited.

We are reachable 24 X 7 on

Email : InternalIS.SecOpsL2Support@tcs.com

Phone : 044 66166324,02263718848,02263718865

Buzz: #04446324,#04278848,#04278865

For any IS Escalations, Please write to internalis.escalation@tcs.com